LINDA LINGLE
GOVERNOR

PATRICIA HAMAMOTO
SUPERINTENDENT

STATE OF HAWAII
DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAII 96804

OFFICE OF THE SUPERINTENDENT

Action Required

December 31, 2009

TO: Assistant Superintendents
Complex Area Superintendents
Principals of Regular and Special Schools

FROM: Patricia Hamamoto
Superintendent

SUBJECT: Privacy and Security of Confidential Student/Employee Data Stored on the Department of Education's Computers

In order to protect confidential student and/or employee information, the Hawaii Department of Education (Department) needs to identify, document and monitor computers hosting confidential student education records or employee data within the schools, complex areas, and state offices. Computers hosting student information or employee data require proper safeguards and procedures to be implemented in compliance with the Family Educational Rights and Privacy Act (FERPA), Board of Education (BOE) policies, and all other privacy laws or regulations. Non-compliance can result in loss of Federal funds, censure and possible legal actions against the Department.

School computers should not be hosting any confidential personally identifiable information (PII) for students or employee data. Department office computers that need to store confidential data should be properly secured, physically and logically (via network access) with the proper procedures in place to control any access to the data.

Our goal is to eventually have all Department computers hosting confidential data situated in a secure data center that meets the highest security and environmental standards. To that end, any school, complex area or state-level offices needing assistance to host confidential data, may request available state-level computers to support this requirement.

Besides computer servers, proper security for desktop/laptop computers should also be practiced. Avoid storing confidential student PII or employee data on desktops or laptops. If one needs to store sensitive data on a desktop or laptop, it should only be for

a temporary timeframe and the attached security guidelines for desktops and laptops should be followed. See Attachment.

Action Required:

1. Identify computers within your facility(ies) that currently host confidential student PII or employee data. If you have no computers hosting confidential student PII or employee data then a "not applicable" response is all that is required.

2. Document the computers that host confidential data:
   a. IP address/computer host name,
   b. location of the computer, and
   c. point of contact.

3. Please email this info to Jeff Hara at jeff_hara@notes.k12.hi.us **by close of business January 28, 2010**.

The Office of Information Technology Services personnel will assist schools, complex area and state-level offices to refine data storage safeguards and procedures in compliance with the Family Educational Rights and Privacy Act (FERPA) and all other privacy laws. Computers hosting confidential data may need to be audited to ensure compliance with proper security standards and privacy laws.

If you have any questions, please contact Mr. Jeff Hara, Office of Information Technology Services, Network Support Services Branch, at 586-3220.

PH:JH:lm

Attachment

c: Board of Education Members
Superintendent's Office Directors
Charter School Administrative Office